



Expert commentary

BS EN ISO 22313:2020 — *Security and resilience — Business Continuity Management Systems — Guidance on the use of BS EN ISO 22301*

Malcolm Cornish, Director, Recovery Management International (UK) Limited



...making excellence a habit.
Documents
Document Sharing Hub

1 Overview

This revision of BS EN ISO 22313:2020 brings it up to date so that it aligns fully with BS EN ISO 22301:2019 *Security and resilience — Business Continuity Management Systems — Requirements*. It uses the same clause numbering and reflects the changes made to that standard during its extensive revision. Whilst BS EN ISO 22301:2019 did not introduce any new requirements, requirements from the previous edition of BS EN ISO 22301 were restated to make them clearer. New terminology was introduced, some familiar terms were eliminated, and the standard was restructured to ensure alignment with Annexe SL, the high-level structure for all ISO management systems standards.

BS EN ISO 22313 casts light on the reasons for the changes made to BS EN ISO 22301, provides clear explanations of technical terms and highlights the difference between requirements relating to the management system and those relating to business continuity management. This edition of the standard will benefit organizations that wish to have an effective business continuity management system and those involved in auditing them.

1.1 Reasons for change

As well as revising BS EN ISO 22313 to reflect changes in the new edition of BS EN ISO 22301, the opportunity was taken to make significant improvements to the guidance. It now provides explanation of business continuity terms that are frequently misunderstood, and the purpose of recommendations is clearly stated. Unnecessary and superfluous detail that could be misleading has been removed.

1.2 Summary:

The most significant changes to BS EN ISO 22313 are as follows:

1.2.1 Revised guidance (see 2.1):

- Determining the scope of the business continuity management system (Clause 4.3)
- Leadership and commitment (Clause 5.1)
- Business continuity objectives and planning to achieve them (Clause 6.2)
- Planning changes to the business continuity management system (Clause 6.3)
- Business continuity management (Clause 8.1.2)
- Business impact analysis (Clause 8.2.2)
- Risk assessment (Clause 8.2.3)
- Business continuity strategies and solutions (Clause 8.3)
- Business continuity plans and procedures (Clause 8.4)
- Performance evaluation (Clause 9)

1.2.2 Guidance resulting from changes to BS EN ISO 22301 (see 2.2)

- Removal of specific requirements
 - Communications
 - Risks
 - Resources
-

2 Main commentary

The next sections explain more about these significant changes.

2.1 Revised guidance

2.1.1 Determining the scope of the business continuity management system (Clause 4.3)

Additional guidance explains the purpose of defining the scope of the management system and identifying valid exclusions. Concerns that inappropriate exclusions might undermine an organization's business continuity are addressed specifically within a new clause 4.3.3. 'Exclusions should not affect the organization's ability to meet business continuity requirements as determined by the business impact analysis (Clause 8.2.2). Activities, resources and supply chains that are required to deliver in-scope products and services cannot be excluded.'

It is expected that organizations ensure that the scope and exclusions (if any) are appropriately defined and that all activities, resources and supply chains required for delivery of in-scope products and services are addressed.

2.1.2 Leadership and commitment (Clause 5.1)

The guidance sets out ways in which top management and other levels of management should demonstrate leadership and commitment and differentiates clearly between the roles of these two levels. Table 3 provides a list of examples of business continuity management system roles and responsibilities.

The revised guidance will be helpful in providing clarity on the meaning of the BS EN ISO 22301 requirements. Organizations should be able to use it to ensure that the allocation of responsibilities is appropriate.

2.1.3 Business continuity objectives and planning to achieve them (Clause 6.2)

The wording in BS EN ISO 22301:2019 has been modified in order to identify clearly the components needed for constructing valid business continuity objectives, and the clause has been split in two (Clause 6.2.1 and 6.2.2) to differentiate between 'establishing' and 'determining' the objectives.

The recommendations in BS EN ISO 22313:2020 have been modified to reflect these changes and new examples of valid business continuity objectives are provided.

It is expected that organizations review the new examples and check that their business continuity objectives include all the recommended components.

2.1.4 Planning changes to the business continuity management system (Clause 6.3)

This clause is new and, in line with other management system standards, has been added to address the need for effective change management controls to be in place. The guidance highlights important aspects that need to be considered.

It could be necessary for organizations to extend their procedures to address this clause.

2.1.5 Business continuity management (Clause 8.1.2)

The term 'Business continuity management' was removed from BS EN ISO 22301 but is retained in BS EN ISO 22313:2020 with a revised definition, which is the only entry in Clause 3 (terms and definitions).

Clause 8.1.2 explains that 'business continuity management' represents Clause 8 in its entirety and identifies the correlation between the elements of business continuity management and each of its clauses. Figure 5 has been updated to show 'Evaluation' as Clause 8.6, the content of which was previously included in Clause 9.1 (see 2.1.10 below)

2.1.6 Business impact analysis (Clause 8.2.2)

The wording in BS EN ISO 22301:2019 relating to the process for analysing business impacts has been revised to set out the requirements more clearly.

The guidance in BS EN ISO 22313:2020 has been rewritten to provide further clarity, particularly in relation to:

- Impact types and criteria
- Timeframes to be used for the analysis and for resumption of activities
- Identification of prioritized activities
- Dependencies and interdependencies of prioritized activities.

The revised guidance also:

- Explains the term 'prioritized activity' and the purpose of identifying prioritized activities
- Suggests high-level approaches for conducting the analysis of business impacts
- Emphasizes that 'terminology used should reflect the way the organization describes its own operations'
- Identifies relationships and dependencies between Clause 8.2.2 and other clauses
- Confirms that the analysis 'should be used to determine business continuity priorities and requirements'
- Sets out additional benefits of the business impact analysis
- Identifies the basis for determining impact types and timeframes
- Identifies the responsibility for determining thresholds of unacceptable impact